IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
ROANOKE DIVISION

In Re Application for a Search Warrant as to the residence of Mike Crowe located at 3653 Daniels Creek Road, Collinsville, Virginia 24078	)	4:20-mj-00019 **By: Hon. Robert S. Ballou** **United States Magistrate Judge**

ORDER

The government filed an application which includes a request for certain biometric searches connected to an individual, Mike Crowe, suspected of violating 18 U.S.C. § 2320(a)(1). The government seeks an anticipatory warrant that will allow the government to enter Mr. Crowe's residence to recover alleged contraband if Mr. Crowe accepts delivery, possession, or control over a package containing such contraband and also takes or moves the package and contraband into the residence. If, upon entering the residence, the government then locates any devices in Mr. Crowe's possession or control protected by his biometric fingerprint or facial recognition profile, the government seeks to be allowed to compel Mr. Crowe to place or swipe his finger on the access readers of such devices or place such devices in front of his face to allow the facial recognition reader to activate.

Touch ID allows an individual to access a device using a fingerprint or thumbprint registered to that device in lieu of a passcode to unlock and use the device. Face ID allows an individual to access a device by allowing it to match the image of their face to a prior scanned image of their face registered to that device in lieu of a passcode to unlock and use the device.

The Touch ID and Face ID features do not work, however, if more than forty-eight hours have passed since the device was last unlocked. Instead, the user can then unlock the device only by inputting the user's passcode.

The warrant application and affidavit stated sufficient probable cause to search electronic devices in Mr. Crowe's possession or control if he takes possession of the contraband and then brings the contraband into his residence. See Riley v. California, 134 S. Ct. 2473, 2493 (2014) (holding that a warrant is generally required before the government can search a cell phone's contents, even if that phone was seized incident to a lawful arrest). The government has sought, as part of its application, to compel Mr. Crowe to apply his finger to unlock the subject devices via Touch ID or place the subject devices in front of his face to use Face ID before the features become disabled.

I cannot compel an individual to reveal the passcode to unlock a phone or other electronic device. See In the Matter of the Search Warrant Application for [redacted text], 279 F.Supp.3d 800, 806 (N.D. Ill. 2017) (explaining that the "principle [articulated by the Supreme Court in Doe v. United States, 487 U.S. 201, 210 n.9 (1988)] applies here: a person generally cannot be compelled to disclose the passcode [to a phone]"); Securities and Exchange Commission v. Huang, No. 15-269, 2015 WL 5611644, at *2–3 (E.D. Pa. Sept. 23, 2015) (holding that the act of producing a personal passcode to a cell phone is testimonial in nature, and thus, a defendant may properly invoke the Fifth Amendment privilege to avoid production of a phone passcode); United States v. Kirschner, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010) (holding that compelling production of password to computer violated Fifth Amendment).

Thus, the government may have no ability to unlock and search the Apple brand devices unless I compel the owner to apply his finger to any such device using Touch ID or place any

such device before his face to allow the Face ID feature to activate. That action, however, may implicate the owner's Fifth Amendment rights. I have reviewed the decision of In the Matter of the Search Warrant Application for [redacted text], which holds that the government can compel a phone owner to provide a fingerprint to unlock an iPhone. 279 F.Supp.3d at 806–807. See also In the Matter of the Search of a White Google Pixel 3 XL Cellphone in a Black Incipio Case, 398 F. Supp.3d 785 (D. Idaho 2019) (same). Other courts, however, have concluded compelling an individual to use a finger or facial features to unlock a device is incriminating testimony within the meaning of the Fifth Amendment. No clear consensus has emerged whether the government's request to use Mr. Crowe's biometric data – either fingerprints or facial recognition – is constitutional. United States v. Warrant, No. 19-mj-71283-VKD-1, 2019 WL 4047615 (N.D. CA August 26, 2019). Because the data on any electronic device may be lost if not unlocked in a timely manner, I will issue the requested warrant and allow the government to compel Mr. Crowe to apply his finger to any such device or have any such device placed in front of his face in an attempt to unlock it.

At this time, the government may only unlock the devices and download or copy the data from them. The government is prohibited from reviewing any of the data from any device which the government unlocked by applying the Mr. Crowe's fingerprint or obtaining the image of Mr. Crowe's face, and must utilize a means to retrieve the data without it being viewed or used by any person involved in the prosecution of the owner of the device or the subject of the search warrant.

It is so **ORDERED**.

Entered: March 21, 2020

Robert S. Ballou

Robert S. Ballou
United States Magistrate Judge